(51) International Patent Classification [7] : H04L 12/56, 12/26, 29/12, 12/14	A1	(11) International Publication Number: **WO 00/56019**
		(43) International Publication Date: 21 September 2000 (21.09.00)

(21) International Application Number: PCT/EP99/01760

(22) International Filing Date: 12 March 1999 (12.03.99)

(71) Applicant *(for all designated States except US)*: NOKIA NETWORKS OY [FI/FI]; P.O. Box 300, FIN–00045 Nokia Group (FI).

(72) Inventor; and
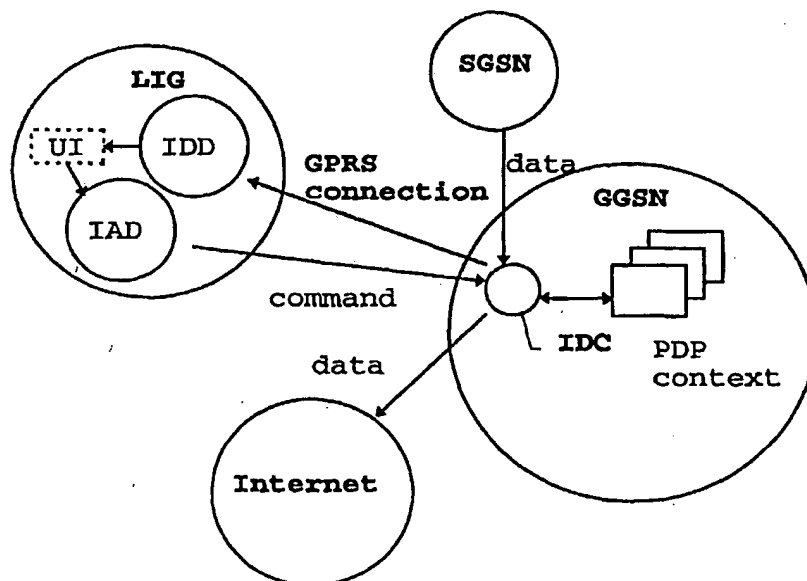(75) Inventor/Applicant *(for US only)*: ELORANTA, Jaana [FI/FI]; Haavikkotie 15–17, FIN–00630 Helsinki (FI).

(74) Agents: PELLMANN, Hans–Bernd et al.; Tiedtke–Bühling–Kinne, Bavariaring 4, D–80336 München (DE).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: INTERCEPTION SYSTEM AND METHOD

(57) Abstract

An interception method and system for performing a lawful interception in a packet network such as a GPRS network is described, wherein a subscriber identity is allocated to an interceptor, such that the interceptor is treated as a mobile station. Thus, the interception traffic is processed as usual data traffic which can be charged using normal charging procedures and which can be intercepted using the normal lawful interception methods. Accordingly, no additional functions are required for charging and intercepting an interception.

Interception system and method

FIELD OF THE INVENTION

5   The present invention relates to an interception system and
method for performing a lawful interception in a packet
network such as the GPRS (General Packet Radio Services) or
the UMTS (Universal Mobile Telecommunications System)
network.

10

BACKGROUND OF THE INVENTION

The provision of a lawful interception is a requirement of
national law, which is usually mandatory. From time to

15   time, a network operator and/or a service provider will be
required, according to a lawful authorization, to make
available results of interception relating to specific
identities to a specific interception authority or Law
Enforcement Agency (LEA).

20

There are various aspects of interception. The respective
national law describes under what conditions and with what
restrictions interception is allowed. If a LEA wishes to
use lawful interception as a tool, it will ask a

25   prosecuting judge or other responsible body for a lawful
authorization, such as a warrant. If the lawful
authorization is granted, the LEA will present the lawful
authorization to an access provider which provides access
from a user's terminal to that network, to the network

30   operator, or to the service provider via an administrative
interface or procedure.

Such a lawful interception functionality is also needed in
the packet switched part of new mobile data networks such

35   as the GPRS and the UMTS.

- 2 -

Several approaches have been proposed so far. According to
the hub approach, a hub is added to the GPRS backbone, such
that all sections will pass through the hub. The benefit of
this system is that the SGSN (Serving GPRS Support Node)
5   and the GGSN (Gateway GPRS Support Node) do not have to
know anything about the lawful interception functionality.
The hub consists of a pseudo GGSN interface and a pseudo
SGSN interface, between which a Lawful Interception Node
(LIN) is arranged.
10

According to another so-called SGSN/GGSN approach, the
whole interception function is integrated into a combined
SGSN/GGSN element. Every physical SGSN/GGSN element is
linked by an own interface to an administrative function.
15   The access method for delivering a GPRS interception
information is based on a duplication of packets
transmitted from an intercepted subscriber via the
SGSN/GGSN element or to another party. The duplicated
packets are sent to a delivery function for delivering the
20   corresponding interception information to the LEA.

Still another approach is to provide an interception or
sniffer element, such as a LIN, in each network segment of
the Ethernet where GPRS data is transferred. The sniffer
25   elements then transmit intercepted data packets to a
collecting LIG (Lawful Interception Gateway) network
element.

In the above hub, SGSN/GGSN and LIN solutions, the
30   intercepted data is transferred independently using an
existing (internal) data network of the network operator.
Thus, an independent charging for interception users has to
be developed.

- 3 -

Furthermore, an interception of another interception
requires an additional method such as auditing a lawful
interception gateway machine by an interception supervisor.

5   Thus, interception charging and interception of
interception is so far not possible without extra effort.

10   SUMMARY OF THE INVENTION

It is therefore an object of the present invention to
provide an interception method and system, by means of
which charging and interception of interception can be
15   easily implemented.

This object is achieved by an interception system for
performing a lawful interception in a packet network,
comprising:
20   interception activation and deactivation means for
allocating a subscriber identity to an interception data
destination in response to the receipt of an interception
request from an interceptor via a user interface; and
interception data collection means for creating a
25   subscriber connection by using said allocated subscriber
identity, in response to an interception activation message
received from said interception activation and deactivation
means, wherein said subscriber connection is used for
transmitting intercepted data to said interception
30   destination.

Furthermore, the above object is achieved by an
interception method for performing a lawful interception in
a packet network, comprising the steps of:

- 4 -

allocating a subscriber identity to an interception data
destination in response to an interception request from an
interceptor;
creating a subscriber connection by using said allocated

5   subscriber identity; and
using said subscriber connection for transmitting
intercepted data to said interception destination.

Accordingly, the intercepted data can be transferred to the

10   interception destination using a normal subscriber
connection. In other words, the interception activation and
deactivation means is emulated as a mobile station. In this
way, the interception activation and deactivation means can
be charged using existing packet network charging

15   functions. However, the billing could have totally
different billing rules for interception users, although
the charging functionality is the same.

Furthermore, the data delivery of intercepted data may also

20   be intercepted, since data and signaling data for an
interceptor will be transferred using a usual subscriber
connection. In this way, any interceptor can be
intercepted.

25   Preferably, the interception activation and deactivation
means are arranged in a legal interception gateway, and the
interception data collection means are arranged in a
gateway GPRS support node (GGSN), wherein said packet
network is a GPRS network. In this case, the subscriber

30   identity is an IMSI address, and the subscriber connection
is a GPRS tunnel. The interception data collection means
may be arranged to create the GPRS tunnel by updating
internal data structures, such as a PDP context, of said
gateway GPRS support node.

35

- 5 -

Thus, it is possible to charge interception authorities
based on the amount of intercepted data, similarly to a
normal GPRS use. Moreover, since any GPRS connection can be
intercepted, a connection carrying intercepted data can be
5   intercepted as well. Thus, legal authorities can supervise
each other.

The interception data collection means may be arranged in
another GPRS network element and adapted to transmit a PDP
10   context creation message to a gateway GPRS support node in
order to create a GPRS tunnel used as the subscriber
connection. In this case, the intercepted data can be
transferred from the GPRS network element to the gateway
GPRS support node by using GTP protocol messages.
15

Preferably, a plurality of predetermined subscriber
identities of the packet network are reserved for the
allocation to interception data destinations. In this case,
an interception hierarchy may be defined on the
20   predetermined subscriber identities, so as to be used to
check whether an interception destination is allowed to
intercept an interception data flow to another interception
destination.

25   Furthermore, the subscriber identity can be allocated, when
a first interception request is received from the
interceptor. The deallocation of the subscriber identity
can be performed, when an interception deactivation request
has been received.
30

Preferably, all interception data and control messages are
transmitted via the subscriber connection. Furthermore, the
subscriber identity may be incorporated in an interception
destination information.
35

- 6 -

BRIEF DESCRIPTION OF THE DRAWINGS

In the following, the present invention will be described
in greater detail on the basis of a preferred embodiment
5   with reference to the accompanying drawings, in which:

Fig. 1 shows a functional block diagram of a lawful
interception system according to the present invention,

10   Fig. 2 shows a general block diagram of an implementation
of a lawful interception system according to the preferred
embodiment of the present invention,

Fig. 3 shows a transmission diagram relating to an
15   interception of a tunnel based on an updating of
interception parameters according to the preferred
embodiment of the present invention, and

Fig. 4 shows a diagram of an implementation of the lawful
20   interception system according to the preferred embodiment
in a GPRS network.

DESCRIPTION OF THE PREFERRED EMBODIMENT

25   In the following, the preferred embodiment of the system
and method according to the present invention will be
described on the basis of a GPRS network.

Fig. 1 shows a functional diagram of a lawful interception
30   for a packet network such as the GPRS network. According to
Figure 1, main functional units of the interception system
are distinguished, such that an implementation in different
real GPRS network elements is possible. According to the
preferred embodiment, different implementation
35   possibilities are available, and the most suitable

implementation must be selected based on the overall GPRS
implementation architecture.

In the following description, a tunnel designates a GTP
5   tunnel between a SGSN and a GGSN, which carries a data
packet belonging to one user connection. User data packets
are called T-PDUs and are carried in G-PDU packets. A
tunnel identifier TID is included in each GTP packet and
contains an IMSI (International Mobile Subscriber Identity)
10 number.

A tunnel activation refers to an activation of a tunnel by
creating a PDP (Packet Data Protocol) context for a user
connection. The SGSN initiates the PDP context creation by
15 sending a Create_PDP_Context_Request message to the GGSN.
The GGSN replies by sending a Create_PDP_Context_Response
message to the SGSN. After a tunnel is activated, user data
is transferred via the tunnel within G-PDU packets, wherein
a G-PDU packet contains a GTP header and user data T-PDU.
20
The tunnel is deactivated by deleting a PDP context earlier
created for a user connection. The SGSN initiates the PDP
context deletion by sending a Delete_PDP_Context_Request
message to the GGSN. The GGSN replies by sending a
25 Delete_PDP_Context_Response message to the SGSN.

The functional diagram shown in Fig. 1 consists of four
functional units. An interception activation monitoring
function IAM monitors the created and deleted tunnels, in
30 order to gather information about the requirement of
activation of any interception in any other functions.
Furthermore, an interception activation and deactivation
function IAD activates and deactivates the current
interception targets, i.e. tunnels, according to an
35 information supplied from the IAM and commands supplied
from a user interface UI in order to change interception

- 8 -

criteria. Additionally, an interception data collection
function IDC is provided, which actually collects the
intercepted data transferred in tunnels and forwards it to
an interception data destination function IDD which
5   receives the intercepted data, probably postprocesses it
and forwards it to the final destination which may be a
representative of some legal authority or a network
operator.

10 Fig. 2 shows a general implementation of the interception
system according to the preferred embodiment in a GPRS
network. The IAD and IDD functions are implemented in a LIG
network element. Moreover, the IAM and IDC functions are
implemented in a gateway GPRS support node GGSN of the GPRS
15 network.

According to the preferred embodiment, intercepted data is
transferred from the IDC function to the IDD function by
using a normal GPRS connection. Thereby, it is possible to
20 charge authorities based on the amount of intercepted data,
similarly to normal GPRS use. Moreover, the GPRS connection
can be intercepted as any GPRS connection.

To achieve this, the IAD function is arranged to allocate
25 and deallocate "fake" IMSI numbers or addresses for
interceptors. These IMSIs are called IIMSIs (Interceptor
IMSIs). These IIMSIs are used for internal GPRS tunnels
that transfer intercepted data. The IIMSI is contained in a
destination information D transferred between the IAD
30 function, the IDC function and the IDD function.

The IAD comprises an interception database which contains
the IIMSIs besides additional interception criteria. The
destination D should uniquely identify an interceptor and
35 its data destination.

In general, the network element including the IAD function
can be located either at the network operator's site or at
the interception authority's site. In the latter case, the
interception authority has total management of it. A

5   problem arises, if several interception authorities manage
their own IAD functions. Namely, because it is possible to
intercept any interception, an interception authority
owning an IAD function could intercept any other
interception authority's interceptions. This problem can be

10   solved by defining an interception hierarchy on the IIMSI
numbers.

For instance, if IMSIs 001-100 are totally reserved to be
used as IIMSIs, then the IAD function can be implemented

15   such that only the numbers 001-020 may intercept the
numbers 21-100. The numbers 021-040 may then be only
allowed to intercept the numbers 040-100, but not the
numbers 001-039. Strict hierarchy is needed in order to
avoid loops in case LEAs are spying each others. The

20   checking operation whether an IIMSI is able to intercept
another IIMSI can be implemented in the IDC function which
is always located at the network operator's site.

Fig. 3 shows a transmission diagram of the transmission of

25   data and messages between the above-mentioned functional
units, wherein the transmission operation starts at the top
of the diagram and moves to the bottom.

The IAM function informs the IAD function of an activated

30   tunnel. However, as long as no interception activation
message has been transmitted from the IAD function to the
IDC function, an interception and collection of the
intercepted data is not performed in the IDC function.
Thus, the first G-PDU packet in Fig. 3 of the activated

35   tunnel TID is not transferred to the IDD function.

- 10 -

Then, an interception activation message is received by the IAD function from the user interface UI. In response to this interception activation message, the IAD function transmits an interception activation message comprising an

5   activation criterion and the allocated IIMSI to the IDC function. In response thereto, the IDC function transmits an activation message comprising the tunnel identification TID and a destination information D comprising the IIMSI to the IDD function, for each tunnel with identifier TID where

10 criterion matches the TID. The criterion can be e.g. an IMSI number, wherein the IDC activates data collection for all tunnels with identifier TID such that TID contains this IMSI. If a G-PDU packet relating to the corresponding tunnel TID is then received by the IDC function, it is

15 collected and transmitted to the IDD function together with the tunnel identification TID and the destination D.

If a deactivation message is received by the IAD from the user interface UI, a corresponding deactivation message is

20 transferred to the IDC function. The IDC then transmits a deactivation message for each tunnel TID which matches the given criterion to the IDD, so as to deactivate the interception operation for this tunnel. The IIMSI is deallocated when a deactivation request for all tunnels of

25 the destination D is received via the user interface UI.

While IIMSI is allocated for an interceptor, several activation and deactivation requests may occur. These requests use the existing IIMSI in the messages transmitted

30 to the IDC function. Similarly, the IAD function passes activation requests to the IDC function every time a tunnel is activated, which should be intercepted using the destination D containing the IIMSI. The tunnel deactivation messages transmitted to the IDD function also contain the

35 IIMSI, since one IDD may receive data for several interception authorities.

- 11 -

The IDC function is the functional unit which actually collects the intercepted data. Thus, the IDC function has to create and delete a GPRS tunnel for the intercepted data
5   transfer from the IDC function to the IDD function. Then, all data and control messages should be transmitted via this GPRS tunnel, instead of the usual data transfer. Accordingly, the IDC function has to know the IIMSI number for each intercepted tunnel.
10

A GPRS tunnel from the IDC function to the IDD function is created either when an interception activation message for a newly generated tunnel or an activation message for a changed interception criterion is received from the IAD,
15   provided that no GPRS tunnel for which an IIMSI already exists is concerned. The GPRS tunnel is deleted when a deactivation message for all interceptions for a destination D is received. Before the tunnel deletion, a corresponding deactivation notification should be
20   transmitted to the IDD function.

As already mentioned, the IDC function has to know the IIMSI for each intercepted tunnel. Then, all intercepted data for this tunnel are transmitted to the correct IDD
25   function using this IIMSI. It is to be noted that also the IDD function knows the IIMSI for each transmitted message, because GTP messages which contain the IIMSI are used for data transfer.

30   Fig. 4 shows an implementation of the interception system according to the preferred embodiment, wherein the IDC function is implemented in a gateway GPRS support node, in line with Fig. 2. In this case, activation and deactivation of the GPRS tunnels can be implemented by updating internal
35   data structures such as a PDP context stored in the GGSN.

- 12 -

If the IDC function is implemented in another GPRS network
element, it has to transmit a PDP_Context_Create or
PDP_Context_Delete message to the GGSN, i.e. it emulates an
SGSN tunnel activation or deactivation.

5

The IDC function in the GGSN receives a G-PDU(TID) data
packet, in case a data is originally transferred in an
intercepted tunnel, e.g. from an SGSN to the Internet, as
shown in Fig. 4. The intercepted data is transferred via
10   the just created GPRS tunnel to the IDD function arranged
in the LIG. The intercepted data is forwarded with the
IIMSI. If the IDC is not included in the GGSN, e.g. in a
SGSN, the intercepted data has to be transferred to the
GGSN using GTP protocol messages.

15

The IDD function in the LIG receives the intercepted data
and transmits it via the user interface UI to the
interceptor to which the IIMSI is allocated.

20   In order to deliver intercepted data, the IDD function in
the LIG just collects all intercepted data belonging to one
destination GPRS tunnel based on the IIMSI which identifies
the interceptor. Thereafter, the IDD function post-
processes the data, removes GTP headers and post-processes
25   data further e.g. on the basis of instructions received
from the interceptor, and delivers the data to its final
destination, e.g. the user interface UI. The IDD function
may collect intercepted data for several interceptors
simultaneously. However, there may also be private IDD
30   functions which serve only one interceptor at a time; in
this case, IDD should be implemented as a separate network
element.

Thus, the preferred embodiment of the present invention
35   presents a general and easy solution for charging and
intercepting interceptions.

- 13 -

It is to be noted that the present invention is not limited
to the described GPRS network and can be used in any packet
network using a subscriber identity for creating a
5   subscriber connection. Thus, the above description of the
preferred embodiment and the accompanying drawings are only
intended to illustrate the present invention. The preferred
embodiment of the invention may vary within the scope of
the attached claims.

10

In summary, an interception method and system for
performing a lawful interception in a packet network such
as a GPRS network is described, wherein a subscriber
identity is allocated to an interceptor, such that the
15   interceptor is treated as a mobile station. Thus, the
interception traffic is processed as usual data traffic
which can be charged using normal charging procedures and
which can be intercepted using the normal lawful
interception methods. Accordingly, no additional functions
20   are required for charging and intercepting an interception.

- 14 -

Claims

1. An interception system for performing a lawful
interception in a packet network, comprising:

5 a) interception activation and deactivation means **(IAD)** for
allocating a subscriber identity to an interception data
destination **(IDD)**; and
b) interception data collection means **(IDC)** for creating a
subscriber connection by using said allocated subscriber

10 identity, in response to an interception activation message
received from said interception activation and deactivation
means **(IAD)**, wherein said subscriber connection is used for
transmitting intercepted data to said interception
destination **(IDD)**.

15

2. An interception system according to claim 1, wherein
said subscriber identity is allocated in response to the
receipt of an interception request from an interception
authority via a user interface **(UI)**.

20

3. An interception system according to claim 1 or 2,
wherein said packet network is a GPRS network, said
interception activation and deactivation means **(IAD)** are
arranged in a legal interception gateway **(LIG)**, and said

25 interception data collection means **(IDC)** are arranged in a
gateway GPRS support node **(GGSN)**.

4. An interception system according to claim 3, wherein
said subscriber identity is an IMSI number and said

30 subscriber connection is a GPRS tunnel.

5. An interception system according to claim 4, wherein
said interception data collection means **(IDC)** is arranged
to create said GPRS tunnel by updating internal data

35 structures of said gateway GPRS support node **(GGSN)**.

- 15 -

6. An interception system according to claim 5, wherein said internal data structure is a PDP context.

7. An interception system according to claim 1, wherein said interception data collection means (IDC) is arranged in a GPRS network element and adapted to transmit a PDP context creation message to a gateway GPRS support node (GGSN) in order to create a GPRS tunnel used as said subscriber connection.

8. An interception system according to claim 7, wherein said intercepted data are transferred from said GPRS network element to said gateway GPRS support node by using GTP protocol messages.

9. A network element for a packet network, comprising:
a) interception activation and deactivation means (IAD) for allocating a subscriber identity to an interception data destination (IDD); and
b) message generation means for generating an interception activation message comprising said subscriber identity and supplying said interception activation message to another network element (GGSN) having an interception data collection function.

10. A network element according to claim 9, wherein said subscriber identity is allocated in response to the receipt of an interception request from an interception authority via a user interface (UI).

11. A network element according to claim 9 or 10, wherein said network element is a lawful interception gateway (LIG) and said another network element is a gateway GPRS support node (GGSN).

12. A network element for a packet network, comprising:

- 16 -

a) interception data collection means **(IDC)** for creating a
subscriber connection by using a subscriber identity
allocated to an interception destination **(IDD)**, in response
to an interception activation message received from another

5   network element **(LIG)** having an interception activation and
deactivation function, said interception activation message
comprising said subscriber identity; and
b) transmitting means for transmitting collected
intercepted data to said interception destination **(IDD)** via

10   said subscriber connection.

13. A network element according to claim 12, wherein said
network element is a gateway GPRS support node **(GGSN)** and
said another network element is a lawful interception

15   gateway **(LIG)**.

14. An interception method for performing a lawful
interception in a packet network, comprising the steps of:
a) allocating a subscriber identity to an interception data

20   destination **(IDD)**;
b) creating a subscriber connection by using said allocated
subscriber identity; and
c) using said subscriber connection for transmitting
intercepted data to said interception destination **(IDD)**.

25

15. An interception method according to claim 14, wherein
said subscriber identity is allocated in response to an
interception request from an interceptor.

30   16. An interception method according to claim 14 or 15,
wherein a plurality of predetermined subscriber identities
of said packet network are reserved for the allocation to
interception data destinations.

35   17. An interception method according to claim 16, wherein
an interception hierarchy is defined on said predetermined

- 17 -

subscriber identities, said interception hierarchy being
used to check whether an interception destination is
allowed to intercept an interception data flow to another
interception destination.

5

18. An interception method according to any one of claims
14 to 17, wherein said subscriber identity is allocated
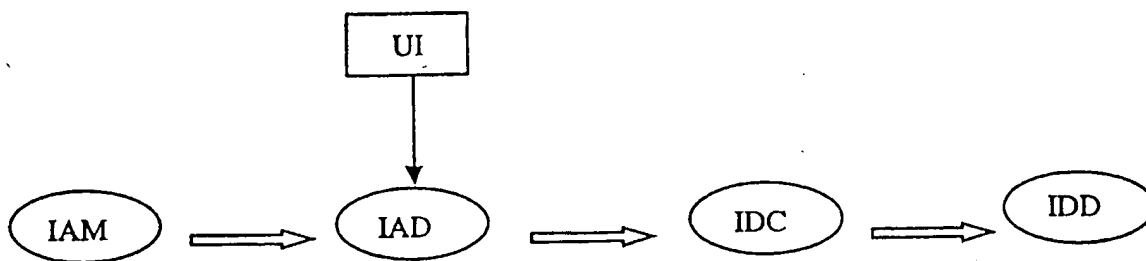when a first interception request is received from said
interceptor.

10

19. An interception method according to any one of claims
14 to 18, wherein said subscriber identity is deallocated
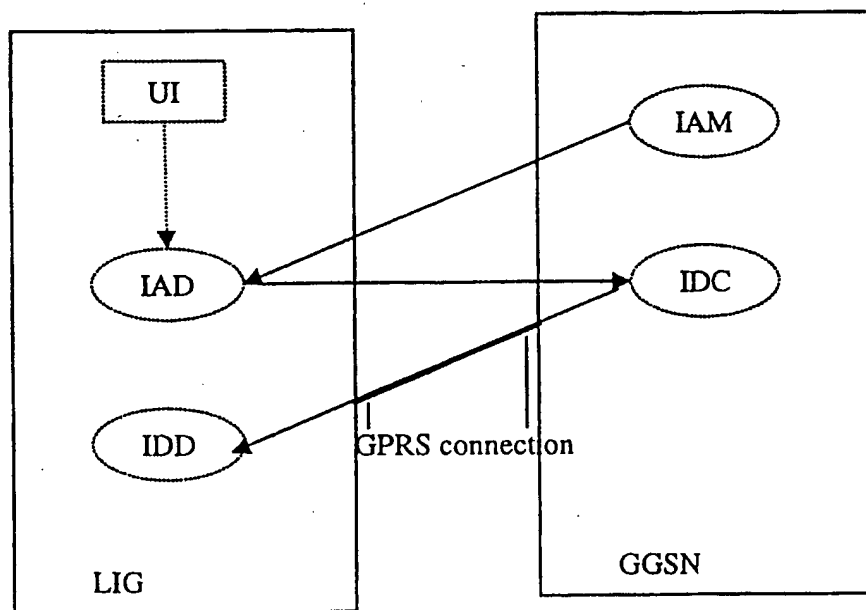when an interception deactivation request has been
received.

15

20. An interception method according to any one of claims
14 to 19, wherein all interception data and control
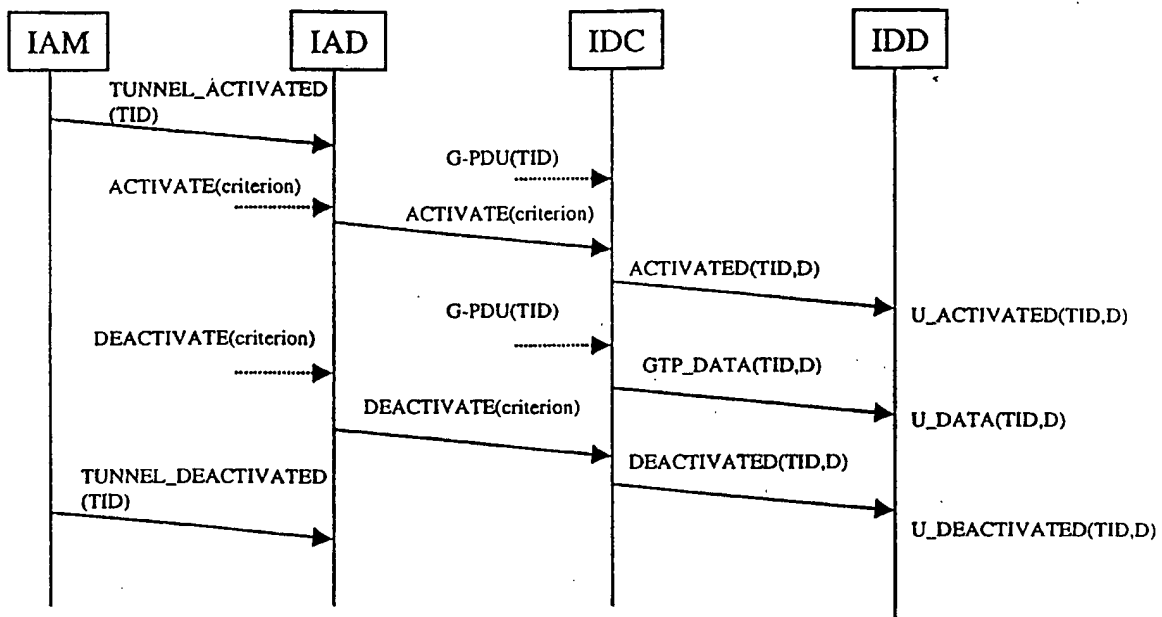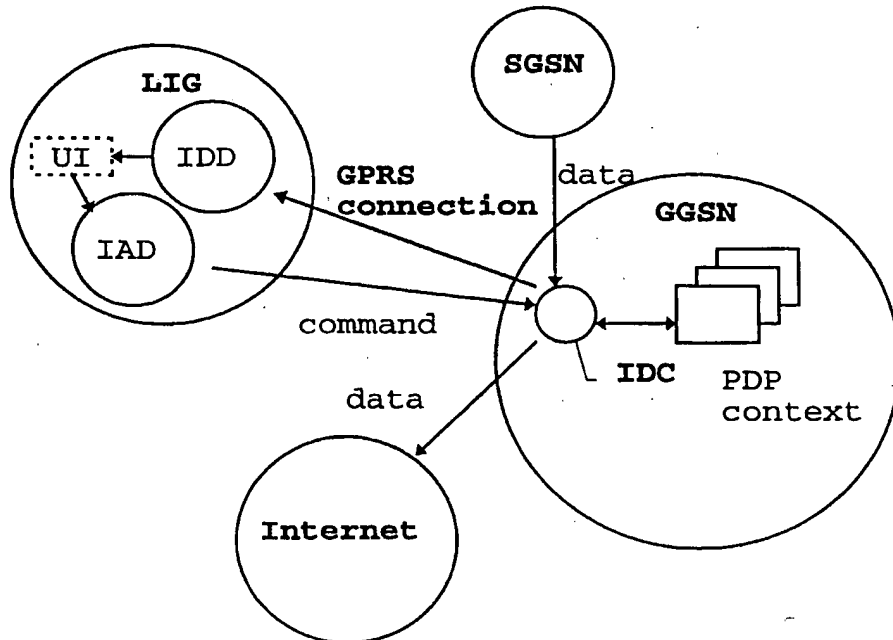messages are transmitted via said subscriber connection.

20   21. An interception method according to any one of claims
14 to 20, wherein said subscriber identity is included in
an interception destination information.

22. An interception method according to any one of claims
25   14 to 21, wherein said subscriber identity is an IMSI
address of a GPRS network, and said subscriber connection
is a GPRS tunnel of said GPRS network.

Fig. 1

Fig. 2

Fig. 3

Fig. 4